(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－83512

(43)公開日　平成９年(1997)３月28日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/20			Ｈ０４Ｌ　9/00	６５３	
Ｇ０９Ｃ　1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６１０Ｄ	
	６５０	7259－5Ｊ		６５０Ｚ	
Ｈ０３Ｋ　19/21		9199－5Ｋ	Ｈ０３Ｋ　19/21		
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全 11 頁）

(21)出願番号　特願平7－239974

(22)出願日　平成７年(1995)９月19日

(71)出願人　000000376
オリンパス光学工業株式会社
東京都渋谷区幡ヶ谷２丁目43番２号

(72)発明者　大山　永昭
神奈川県横浜市緑区長津田町4259　東京工業大学内

(72)発明者　小宮　康宏
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内

(72)発明者　小俣　芳信
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内

(74)代理人　弁理士　鈴江　武彦

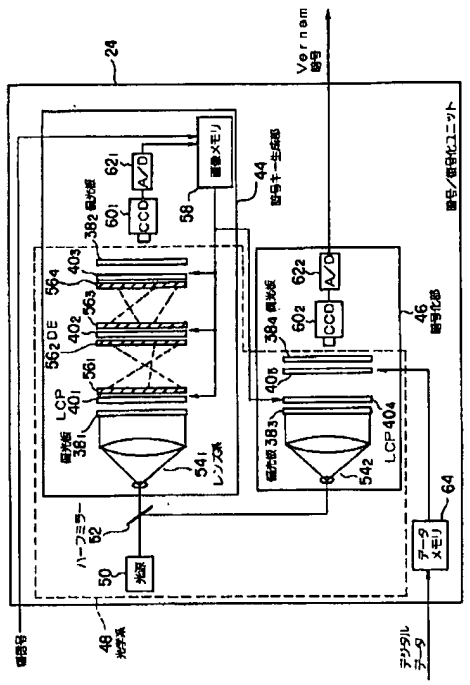
最終頁に続く

(54)【発明の名称】　暗号化システム及びそれに利用可能な光学的排他的論理和演算装置

(57)【要約】

【課題】Vernam暗号を高速に処理できるようにすること。

【解決手段】暗号化キー生成部４４の偏光板３８１，３８２、液晶パネル（ＬＣＰ）４０１～４０３、回折素子（ＤＥ）５６１～５６４は、各ＬＣＰの各画素間の３ビットの演算を行う光学的排他的論理和演算装置を構成する。ＤＥは演算すべき各画素間の対応を導く。ＬＣＰ４０１には、初期値ベクトル（最初は種信号）に対応するパターンが表示される。偏光板３８３からの出力光を撮像しＡ／Ｄ変換することで、ＬＣＰの画素に対応したランダムなビット列が暗号化キーとして得られる。これが、暗号化部４６の偏光板３８３，３８４、ＬＣＰ４０４，４０５でなる光学的排他的論理和演算装置のＬＣＰ４０４に表示され、また暗号化されるべきデジタルデータがＬＣＰ４０５に表示される。偏光板３８４からの出力光は、撮像され、Ａ／Ｄ変換されて、Vernam暗号として出力される。



[Document Name] Description

[Title of the Invention] An encryption system and optical exclusive OR operation equipment available to it

[Claim(s)]

[Claim 1] The digital data which should be enciphered as the cryptographic key formation part which generates a cryptographic key in response to a seed signal, or the enciphered digital data is received. In the encryption system equipped with encryption/decoding part which consists of an exclusive OR operation part which outputs the digital data which performed the exclusive OR operation of this digital data and the cryptographic key generated in said cryptographic key formation part, and was enciphered, or the decrypted digital data Either [at least] said cryptographic key formation part or said exclusive OR operation part is the encryption system characterized by including the optical exclusive OR operation equipment using a spatial modulation element.

[Claim 2] The optical exclusive OR operation equipment of said cryptographic key formation part V(x) =1+xk+xn The encryption system according to claim 1 characterized by being constituted so that a false random number with the n bit maximum length series sign based on the primitive polynomial expressed with (n>k>n/2) may be generated. [however,]

[Claim 3] Optical exclusive OR operation equipment characterized by providing the spatial modulation element of two or more sheets which aligned with said polarizing plate, respectively and was arranged between two polarizing plates and these polarizing plates.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the encryption system in Digital Communications Division etc., and optical exclusive OR operation equipment available to it.

[0002]

[Description of the Prior Art] In the digital communication network of a highly information-oriented society, in order to secure the safety of information, various kinds of encryption techniques are becoming important.

[0003] It is divided roughly into two, although it is large to a cipher system and a secret key (it is also called a common key) is used for it with the thing using a public key. Especially the latter secret key also has a role like a seal in a communications network, and it is thought that it will be used increasingly from now on.

[0004] The VANAMU (it is hereafter described as Vernam) code which calculates the exclusive OR (it is hereafter described as XOR) of a random key and random **** (data to encipher) as a technique using a secret key, and is enciphered is known. Generally in this Vernam code, the false random number which used the initial value of a certain length as the seed is used as a cryptographic key.

[0005] (B) of drawing 8 is drawing showing the algorithm of the Vernam code which used the maximum length series sign (an M sequence is called hereafter) as birth of a false random number.

[0006] In this drawing, the reference number 1A is digital data (equivalent to ****) to encipher, and this is given to the encryption part 2A. The encryption part 2A consists of XOR circuit 5A which performs the XOR operation of the cryptographic key formation part 4A which generates an M sequence random number as a cryptographic key, and this cryptographic key and above-mentioned digital data 1A that were generated by making the seed signal 3A into an initial value, and outputs that XOR operation result as a Vernam code.

[0007] The Vernam code outputted from this encryption part 2A is sent to decoding part 2B through a transmission line 6.

[0008] The cryptographic key formation part 4B which decoding part 2B has the same composition as the above-mentioned encryption part 2A, and generates an M sequence random number as a cryptographic key from the seed signal 3B, It consists of XOR circuit 5B which performs the XOR operation of this generated cryptographic key and the transmitted Vernam code, and outputs as digital data 1B which had the XOR operation result decrypted.

[0009] Since this Vernam code is a secret key method, the above-mentioned seed signal 3A and the seed signal 3B are the same signals.

[0010]

[Problem to be solved by the invention] It is shown clearly that a Vernam code is a code method with high safety when a huge cryptographic key is used. In this Vernam code, as mentioned above, the false random number which used the initial value of a certain length as the seed is used as a cryptographic key, but it depends for the cycle of such a random number on the size of the signal (signal kind) used as a seed. Therefore, in order to secure high safety

in a Vernam code, it is necessary to generate a false random number huge as a cryptographic key.

[0011] However, in order to maintain sufficient safety to encipher mass data like a picture and to generate such a huge false random number When requiring very many computational complexities and enciphering or decrypting mass data by computers, such as a personal computer (it abbreviates to a personal computer hereafter), it had the trouble of taking time very.

[0012] This invention was made in view of the above-mentioned point, and aims at providing with available optical exclusive OR operation equipment the encryption system and it which can process a Vernam code at high speed.

[0013]

[Means for solving problem] [the encryption system by this invention] in order to attain the above-mentioned purpose The digital data which should be enciphered as the cryptographic key formation part which generates a cryptographic key in response to a seed signal, or the enciphered digital data is received. Are encryption/decoding part which consists of an exclusive OR operation part which outputs the digital data which performed the exclusive OR operation of this digital data and the cryptographic key generated in said cryptographic key formation part, and was enciphered, or the decrypted digital data the encryption system which it had, and especially Either [at least] said cryptographic key formation part or said exclusive OR operation part is characterized by including the optical exclusive OR operation equipment using a spatial modulation element.

[0014] That is, according to the encryption system of this invention, in order to encipher mass data, the false random number which made the comparatively big data of a picture etc. the seed signal is generated as a cryptographic key. At this time, it is made to perform formation of a cryptographic key or encryption of digital data, and a decoding using the optical exclusive OR operation equipment which used the spatial modulation element as an optical parallel operation system paying attention to the ability of light to treat mass information in parallel.

[0015] Moreover, the optical exclusive OR operation equipment by this invention is characterized by having the spatial modulation element of two or more sheets which aligned with said polarizing plate, respectively and was arranged between two polarizing plates and these polarizing plates.

[0016] That is, while adjusting the polarization direction of a polarizing plate, it enables it to carry out the exclusive OR operation for several of the area minutes in parallel by controlling the abnormal-conditions state of the area corresponding to each digital data of each spatial modulation element arranged among them according to the optical exclusive OR operation equipment of this invention.

[0017]

[Mode for carrying out the invention] The form of operation of this invention is hereafter explained with reference to Drawings.

[0018] [Form of the 1st operation] Drawing 2 is drawing showing the composition of the encryption system in the form of operation of the 1st of this invention, and the reference numbers 10A and 10B are communication terminals, such as a personal computer, in this drawing. 12A and 12B are storages, such as a hard disk and a magneto-optical disc, and these storages 12A and 12B memorize the digital data 14A and 14B which is the data which should be enciphered, or decrypted data. This digital data 14A and 14B may be data like a throat of a picture, a sound, text data, etc., etc. Furthermore, the storages 12A and 12B have memorized seed signal a16A, 16B, seed signal b18A, 18B, seed signal c20A, and 20B. Here, although seed signal a-c as a kind which generates a huge key assumes the case where it is image data, if a text etc. is digital data, of course, anything may be used for it.

[0019] Such storages 12A and 12B are connected to a code / decoding modules 24A and 24B and RAM26A, and 26B through data buses 22A and 22B. A code / decoding modules 24A and 24B have the function which enciphers digital data to a Vernam code, or decodes a Vernam

code to digital data conversely so that it may explain in detail later. Moreover, the control programs 28A and 28B for RAM26A and 26B to control encryption, a decoding, and communication by CPU which is not illustrated are read.

[0020] And further, the communications control machines 30A and 30B, such as a modem, are connected to data buses 22A and 22B, and the Vernam code enciphered in a code / decoding modules 24A and 24B among them is transmitted to them through the transmission line 32 for communication.

[0021] Here, although a code / decoding module 24A, and 24B per explanation are given, in order to help the understanding, after being engaged in birth of a false random number, description is started first.

[0022] An M sequence is a code word generated using a linearity shift register circuit (LSR is called hereafter), and is a series random in false. If the shift register of n stage is used, it is known that a series with 2n of cycles of -1 can be generated. When this n is chosen suitably, it is V(x) =1+xk+xn. (n, k: positive integer) A 1 bit [per one clock] series is generated by the circuit as shown in (A) of drawing 3 based on primitive polynomial V (x) expressed. Here, it is xk. It means applying feedback from the register of eye k stage in LSR34. attaching to each bit of LSR34 the number from 1 (bit generated last time) to n (bit generated n times ago) in this drawing -- a1 from -- an expressing -- a0 Signs that a new bit is generated are shown. What carried out the XOR operation of the n-th bit and the k-th bit by XOR circuit 36 in the example of this primitive polynomial is a0. It becomes. In this way, a0 After being generated, it is this a0. a1 Since it carries out and all the bits are shifted, it is old an. It is lost. A bit string random in false is generated by repeating this operation.

[0023] The M sequence can generate n series at once to n initial inputs by using the conversion in the state after n clock shift from a certain state. Furthermore, if its attention is paid when it is n>k>n/2, formation of n series is simultaneously possible by combining exchange of a bit, and a maximum of 3-bit XOR.

[0024] Here, the case of n= 10 and k= 7 is concretely explained using (B) of drawing 3. The

number of each column in this drawing shall correspond to the bit value of an initial value, and a sign "^" shall express a XOR operation. Moreover, each line shows the state of each bit when generating 1 bit of random number sequences at a time from an initial value. This drawing shows that each bit state after 10 clock shift is equivalent to ten random number sequences. Moreover, it turns out that the state after 10 clock shift is realized by a maximum of 3-bit XOR.

[0025] (C) of drawing 3 is the key map of the connection which can generate the random number sequence of n bit at a time as mentioned above. This connection consists of three layers, the input (the 1st layer) of a connection is the initial value vector a, the 2nd layer and 3rd-layer inputs are b and c, and outputs are bout and cout. It is. Moreover, cout It is also the output of this connection and becomes the random number sequence of n bit. bout Are the XOR operation of a and b and it is cout. A result of the XOR operation of a' and c is brought.

[0026] When a= (a1, a2, --, an), b here bi =ai+n-k (i<=k), bi =ai-k (i>k) -- It is expressed (1) and c is ci =bi+n-k out. (i<=k) ci =bi-k out (i>k) -- It is expressed (2). Moreover, a' is a'i =ai. (2 k-n<i<=k) a'i =0 (2 k-n>=i, i>k) -- It is expressed (3).

[0027] Here, in (B) of drawing 3, in the line behind 10 clocks, a'i =0 has the place which takes two XOR and three XOR, and it shows the place which has taken these two XOR. That is, it can be considered that this portion has taken XOR of "0."

[0028] And output cout of this connection The following n bit random number can be generated by considering it as the initial value vector a anew. Even if it makes the connection of this each layer reverse, the turn of a random number sequence changes, but the same effect is acquired.

[0029] If the two or more bits parallel XOR operation performed by such 2nd layer, the 3rd layer, etc. is realizable, encryption can be performed at high speed.

[0030] With the form of this operation, the optical system using a spatial modulation element as shows such a parallel XOR operation to (A) of drawing 4, i.e., optical exclusive OR operation equipment, has realized. In addition, in the form of this operation, although a liquid crystal panel is explained to an example as a spatial modulation element, as for this invention, it is needless to say that it is not limited only to it.

[0031] In this drawing, the reference numbers 38A and 38B are polarizing plates, and they are arranged so that a mutual plane of polarization may become right-angled. And the liquid crystal panels (LCP is called hereafter) 40A and 40B of homogeneous orientation are arranged in the meantime. Moreover, 42 expresses the output screen. In addition, in LCP40A, 40B, and an output screen 42, this drawing shows only 4 pixels for simplification.

[0032] In such an optical system, a XOR operation is attained by controlling LCP40A and 40B as 1/2 wave plate per stroke matter. That is, since LCP40A and 40B work as 1/2 wave plate in the state of ON (the white pixel a, b, and c all over drawing, d), as a both-directions arrow shows all over drawing, they can change a polarization direction 90 degrees to incident light. Moreover, in OFF (black pixel a' all over drawing, b', c', d'), the polarization direction of incident light does not change. Therefore, when [both] both LCP40A and LCP40B are ON (pixel e), and when it is OFF (pixel f), an output screen 42 serves as OFF, but when only one of LCP40A and the LCP40B is ON (pixels g and h), an output screen 42 is set to ON and can realize a XOR operation.

[0033] As for this operation, each pixel of LCP is equivalent to 1 bit, and the XOR operation for a pixel number of LCP can be performed simultaneously. In addition, a XOR operation of 3 bits or more increases the number of LCP(s) set among polarizing plates 38A and 38B, is changing the polarization direction by a polarizing plate suitably, and becomes possible.

[0034] Using such an optical system, above-mentioned code / decoding modules 24A and 24B are constituted, for example, as shown in drawing 1.

[0035] That is, each is realized by the optical system 48 although the code / decoding module 24 as above-mentioned code / decoding modules 24A and 24B consist of a code key generation part 44 and an encryption part 46. For example, the coherent light from the luminous sources 50, such as laser, branches with a half mirror 52, and is led to the cryptographic key formation part 44 and the encryption part 46.

[0036] In the cryptographic key formation part 44, it is the lens system 541 about incidence coherent light. Polarizing plate 381 after making it a parallel beam It is led. This polarizing plate 381 LCP401, 402, 403, the diffraction element (diffraction element:DE is called hereafter) 561, 562, 563, 564, and polarizing plate 382 The connection mentioned above is realized. Here, it is DE561, 562, 563, and 564. Light is bent towards desired and this is realized by the hologram etc., for example. Namely, DE561 and 563 LCP401 and 402 It bends and acts as Idei of the light parallel to the optical axis which came out through each pixel towards desired for every pixel. DE562 and 564 DE561 and 563 from -- returning light in the direction parallel to an optical axis -- LCP402 and 403 The duty to enter is achieved.

[0037] here -- LCP401 **** -- the pattern corresponding to the initial value vector memorized by the image memory 58 is displayed. In addition, this initial value vector is the seed signal which was read from the storage 12A or 12B, and was stored temporarily at first at the image memory 58. and polarizing plate 381 from -- output light -- CCD camera 601 picturizing -- A/D conversion part 621 The random bit string corresponding to the pixel of LCP is obtained by carrying out through and suitable threshold processing. In addition, the threshold processing circuit is not illustrated. This bit string is memorized by the image memory 58, and it is inputted into the encryption part 46 as a cryptographic key while being fed back again, in order to generate the following random bit string.

[0038] In the encryption part 46, it is this inputted cryptographic key LCP404 It displays. On the other hand, as for the digital data which should be enciphered, it is read from the storage 12A or 12B, the data memory 64 memorizes, and this is LCP405. It is displayed. polarizing plate 383 **** -- the light which branched by the above-mentioned half mirror 52 -- lens system 542 it having been made the parallel beam and having entered -- LCP404 and 405 A polarizing plate 383 and 384 A XOR operation is performed as mentioned above. polarizing plate 384 from -- output light -- CCD camera 602 being picturized -- A/D conversion part 622 It is changed into digital data and this is outputted as a Vernam code. Threshold processing is carried out also in

this case, and it outputs as a bit string.

[0039] Here, in accordance with the total number of bits (N) of a seed signal, the total number of bits (M) of digital data to encipher does not need to feed back, when the seed signal is larger (M<=N), but since it is generally M>N, feedback is performed.

[0040] In addition, in such the code / a decoding module 24 of composition, in decrypting a Vernam code, it passes the data memory 64, and it is a Vernam code instead of digital data LCP405 What is necessary is just to make it display. Thereby, it is the A/D conversion part 622. The digital data decrypted by the output is obtained.

[0041] In the encryption system of the above composition, it operates as follows. In addition, although communication of the code in both directions of the communication terminals 10A and 10B can be performed, the case where the Vernam communication enciphered from the communication terminal 10A to the communication terminal 10B here is sent is explained.

[0042] First, in the communication terminal 10A, the control program for communication is started and this is read into RAM26A. Next, while specifying the digital data 14A to transmit, the seed signal used for encryption is specified. Here, suppose that for example, seed signal b18A was chosen. This digital data 14A and seed signal b18A are decoding module 24A [a code /] Sent, and a Vernam signal is generated by the processing mentioned above. Through the communications control machine 30A, this Vernam signal passes along a transmission line 32, and is sent to the communication terminal 10B. In the communication terminal 10B, while the Vernam signal inputted is sent to a code / decoding module 24B through the communications control machine 30B, seed signal b18B is read and it is sent to a code / decoding module 24B. And it is decrypted as original digital data. In addition, by the seed signals a and the seed signals c other than the seed signal b, the decoding to the original digital data cannot be performed with a natural thing at the time of this decoding, but it is necessary to use the same seed signal b as the time of using for encryption.

[0043] With the form of this operation, processing of the encryption using a huge key and a decoding can be performed at very high speed as mentioned above by using optical exclusive

OR operation equipment for a code / decoding module. And if there is 400,000 pixels of LCD etc., encryption for 400,000 bits can be performed in once.

[0044] In addition, although DE (diffraction element) is arranged to in-line one with the composition of drawing 1, it is also possible to make it offset from an optical axis, of course, and to arrange.

[0045] Moreover, as shown in drawing 5, it is the optical fiber (all over drawing, it is described as OF) 661, and 662 instead of a diffraction element. The connected module is also realizable. In this case, as a luminous source 50, as long as a wavelength band is narrow enough, you may not generate coherent light.

[0046] Moreover, as shown in (B) of drawing 4, a code / decoding module 24 may be made to be incorporated into the communications control machine 30.

[0047] At the form of this operation, it is CCD camera 601 and 602 to read-out of a signal. Although used, LCLV (Liquid Crystal Light Valve) can also be used. In this case, output light by the side of the code key generation part 44 can be directly considered as the input for a XOR operation part of the encryption part 46 through an optical system.

[0048] Furthermore, the technique called spatial coding can also be used as a method of realizing a XOR operation optically.

[0049] [Form of the 2nd operation] Next, the form of the operation of the 2nd of this invention which increased a transmission rate and safety further is explained with reference to drawing 6.

[0050] With the form of implementation of the above 1st, the Vernam code was transmitted in the transmission line 32. When using the telephone line of 2400BPS for this transmission line, for example and sending the Vernam code of the RGB color picture data of 512 pixels of each

every direction to it, it will take (512*512*3*8) / (2400*60) = no less than 43.69 minutes. When there is two or more data to process, transmission by the present telephone line is not realistic.

[0051] Then, he memorizes a Vernam code to an external storage, and is trying to convey off-line in the form of this operation.

[0052] That is, in drawing 6, the reference numbers 68A and 68B are the 1st data input/output equipment, for example, are a floppy disk drive and an optical magnetism disk drive. A Vernam code is memorized by the storages 70, such as a floppy disk and a magneto-optical disc, and off-line conveyance is carried out.

[0053] Moreover, in the form of implementation of the above 1st, although the seed signal was beforehand memorized by the communication terminal, since a decoding can be tried on all the seed signals, there is room of the further improvement in this case, in the meaning which increases safety more.

[0054] So, with the form of this operation, it proposes storing a seed signal in media other than a communication terminal. That is, in this drawing, the reference numbers 72A and 72B are the 2nd data input/output equipment, for example, are IC card reader writer and an optical card drive. And a seed signal is memorized by the portable storage 74 of an IC card, an optical card, etc., and off-line conveyance is carried out. Here, in order to maintain the safety of information, the individual using data carried, it is [direction] good and the point, and an IC card (especially since CPU is included, privacy is high) and an optical card convenient to carry are effective, although a floppy disk, a magneto-optical disc, etc. may be made to memorize a seed signal. Moreover, when only two or more members who share a secret mutually in this case have the storage of the same seed signal, the safety of information is secured more highly.

[0055] [Form of the 3rd operation] Still more above code / decoding modules 24 of composition are not necessarily required for each terminal 10. As shown in drawing 7 in recent years, an opportunity to connect each terminal by network by LAN is increasing, but the protecting wall

called a gateway 78 to the portion linked to the external communications network 76 may be installed in that case. Then, the enciphered data can be used, only when installing in a gateway 78 rather than forming a code / decoding module 24 in each terminal 10 and performing exchange of the exterior and data.

[0056] When it has such composition, in utilization of medical data etc., it is effective. Namely, except that a certain patient needs to start and it attaches, when it is taken to a hospital (for example, an emergency hospital; LAN2 in drawing 7 are employed), When the doctor of the carried hospital wants to know the patient's old appearance, It is in the place which the patient left using the card which memorized the learned seed signal, the database (LAN1 in drawing 7 is employed) of the hospital of the price can be accessed, and the data of a wish can be got safely. This patient's data cannot be seen as long as there is no card which memorized the seed signal, but privacy is kept perfect.

[0057] Of course, as shown in drawing 7, you may install a code / decoding module 24 in the gateway / terminal 80 at the entrance of a subnetwork. Many [-fold] can be enciphered by doing in this way. for example, if a subnetwork is built for two or more of its posts of every in a certain building connected by LAN, when data will be transmitted by **** within the station and the data will be passed to its posts of other It can encipher and pass in the code / decoding module 24 installed in the gateway / terminal 80. Furthermore, ** which can increase more the privacy of the data transmitted outside since it can encipher once again in the code / decoding module 24 installed in the gateway 78 when transmitting it outside a building through the external communications network 76

[0058] [Form of the 4th operation] A seed signal is used for the form of this operation instead of the seal in digital data. That is, in the present public seal registration, what printed out the sealed shade and the registered shade is compared and checked. However, to digital data, what hits a seal is not put in practical use by the present.

[0059] Then, as shown in (A) of drawing 8, the data which took in with the scanner etc. the shade proved or registered publicly is made into the seed signal for key generation, and if it is not the shade proved by the public register when enciphering data to prove, can decrypt data and it cannot be used. A seed signal can be used instead of a seal by the thing for which this

seed signal was mentioned above and which it memorizes to the IC card and is done for a code/decoding as stated in the form of the 2nd operation.

[0060] In addition, if the seed signal registered in this case is data proved publicly [a seal a signature, etc.], its thing good [anything] is natural.

[0061] [Form of the 5th operation] A picture can be used as a seed signal for generating the encryption key described with the form of the above 1st or the 4th implementation. Generally, since capacity of image data is large, it is suitable as a seed signal which generates a huge key. Moreover, generally, since image data is expressed as gray scale data with 1-pixel a 8-bit tone wedge, for example, as it was called the 3rd bit of each pixel high order, it can use the bit slice of each pixel value as a seed signal. Or it is also possible to choose the bit string of the picture which thinned out original image data as a seed signal.

[0062] Of course, the code/decoding in this invention are **/reception sides of the data of a code, and since what is necessary is just to use the same seed signal, naturally [although two kinds were mentioned as a method of choosing a seed signal from image data with the form of this operation] selection of the seed signal except having mentioned here is possible.

[0063] Although this invention was explained based on the form of operation above, this invention is not limited to the form of operation mentioned above, and various modification and application are possible for it within the limits of the summary of this invention. Here, it is as follows when the summary of this invention is summarized.

[0064] (1) The cryptographic key formation part which generates a cryptographic key in response to a seed signal, The digital data which should be enciphered, or the enciphered digital data is received. In the encryption system equipped with encryption/decoding part which consists of an exclusive OR operation part which outputs the digital data which performed the exclusive OR operation of this digital data and the cryptographic key generated in said cryptographic key formation part, and was enciphered, or the decrypted digital data Either [at least] said cryptographic key formation part or said exclusive OR operation part is the encryption system characterized by including the optical exclusive OR operation equipment

using a spatial modulation element.

[0065] Namely, in order to encipher mass data, while generating the false random number which made the comparatively big data of a picture etc. the seed signal as a cryptographic key At this time, the optical exclusive OR operation equipment using the spatial modulation element as an optical parallel operation system is used paying attention to the ability of light to treat mass information in parallel. At very high speed, since it is made to perform formation of a cryptographic key, or encryption of digital data, processing of the encryption using a huge key and a decoding can be performed.

[0066] The optical exclusive OR operation equipment of said cryptographic key formation part (2) V(x) =1+xk+xn An encryption system given in (1) characterized by being constituted so that a false random number with the n bit maximum length series sign based on the primitive polynomial expressed with (n>k>n/2) may be generated. [however,]

[0067] That is, the number of the spatial modulation element used for the optical exclusive OR operation equipment can be made into the minimum with constituting optical exclusive OR operation equipment based on the above-mentioned primitive polynomial.

[0068] (3) Optical exclusive OR operation equipment characterized by providing the spatial modulation element of two or more sheets which aligned with said polarizing plate, respectively and was arranged between two polarizing plates and these polarizing plates.

[0069] That is, while adjusting the polarization direction of a polarizing plate, the exclusive OR operation for several of the area minutes can be carried out in parallel by controlling the abnormal-conditions state of the area corresponding to each digital data of each spatial modulation element arranged among them.

[0070] (4) Said seed signal is memorized by the storage which can be freely detached and attached on the main part of equipment which holds said encryption/decoding part, and [said encryption/decoding module] An encryption system given in (1) characterized by including a

means to read a seed signal from said storage and to supply said cryptographic key formation part.

[0071] That is, it cannot have a seed signal in the main part of equipment which holds encryption/decoding part, but the secret nature of digital data or a code can be improved more because a specific person makes it memorize in the storage in which a form is possible.

[0072] (5) Said seed signal is an encryption system given in (1) characterized by being data proved publicly.

[0073] Namely, a seed signal can be used now instead of a seal.

[0074] (6) Said seed signal is an encryption system given in (1) characterized by being a picture signal with a tone wedge.

[0075] That is, since capacity of image data is large, it is suitable as a seed signal which generates a huge key. Moreover, since it is also possible to use a part of image data for a seed signal Since the data enciphered even if the image data came to hand unjustly cannot be decrypted unless there is no telling which portion of image data is chosen with the seed signal, the secret nature of digital data or a code can be improved.

[0076] (7) Said encryption/decoding part is an encryption system given in (1) characterized by being in the portion of the input/output part of the information in the predetermined area in an information network by which the grouping was carried out.

[0077] Namely, in the predetermined area in an information network by which the grouping was carried out Since what is necessary is just to encipher/decrypt, even if each terminal does not have encryption/decoding part, it becomes possible to exchange the data enciphered as the Eria exterior from every terminal, and it can improve the privacy of information with the simplification of an entire configuration.

[0078]

[Effect of the Invention] As explained in full detail above, according to this invention, the encryption system and it which can process a Vernam code at high speed can be provided with available optical exclusive OR operation equipment.

[Brief Description of the Drawings]

[Drawing 1] It is the block block diagram of the code / decoding module in the form of the 1st operation.

[Drawing 2] It is the block block diagram of the encryption system in the form of the 1st operation.

[Drawing 3] It is drawing showing a bit state when drawing showing a false random-number-generation circuit with the n bit maximum length series sign (M sequence) which used the linearity shift register circuit, and (B) set (A) to n= 10 and k= 7 in (A), and (C) is the key map of the connection which can generate the random number sequence of n bit at a time.

[Drawing 4] (A) is drawing for explaining the principle of the optical exclusive OR equipment in the form of the 1st operation, and (B) is the block block diagram showing the modification of the encryption system in the form of the 1st operation.

[Drawing 5] It is the block block diagram showing the modification of the code / decoding module in the form of the 1st operation.

[Drawing 6] It is the block block diagram of the encryption system in the form of the 2nd

operation.

[Drawing 7] It is drawing showing the composition of the encryption system in the form of the 3rd operation.

[Drawing 8] (A) is drawing for [which uses a seed signal as a digital seal] explaining the form of the 4th operation, and (B) is the block block diagram of the conventional encryption system.

[Explanations of letters or numerals] 10, 10A, 10B -- Communication terminal 14A, 14B -- Digital data, 16A, 16B -- Seed signal a 18A, 18B -- Seed signal b 20A, 20B -- Seed signal c 24, 24A, 24B -- A code / decoding module 30, 30A, 30B -- Communications control machine, 32 -- Transmission line 38A, 38B, and 381-384 -- Polarizing plate, 40A, 40B, and 401-405 -- Liquid crystal panel (LCP) 44 -- Cryptographic key formation part, 46 -- Encryption part 561-564 -- Diffraction element (DE) 661 and 662 -- Optical fiber (OF) 68A, 68B, 72A, 72B -- Data input/output equipment 70, 74 -- Storage 78 -- Gateway 80 -- A gateway/terminal.

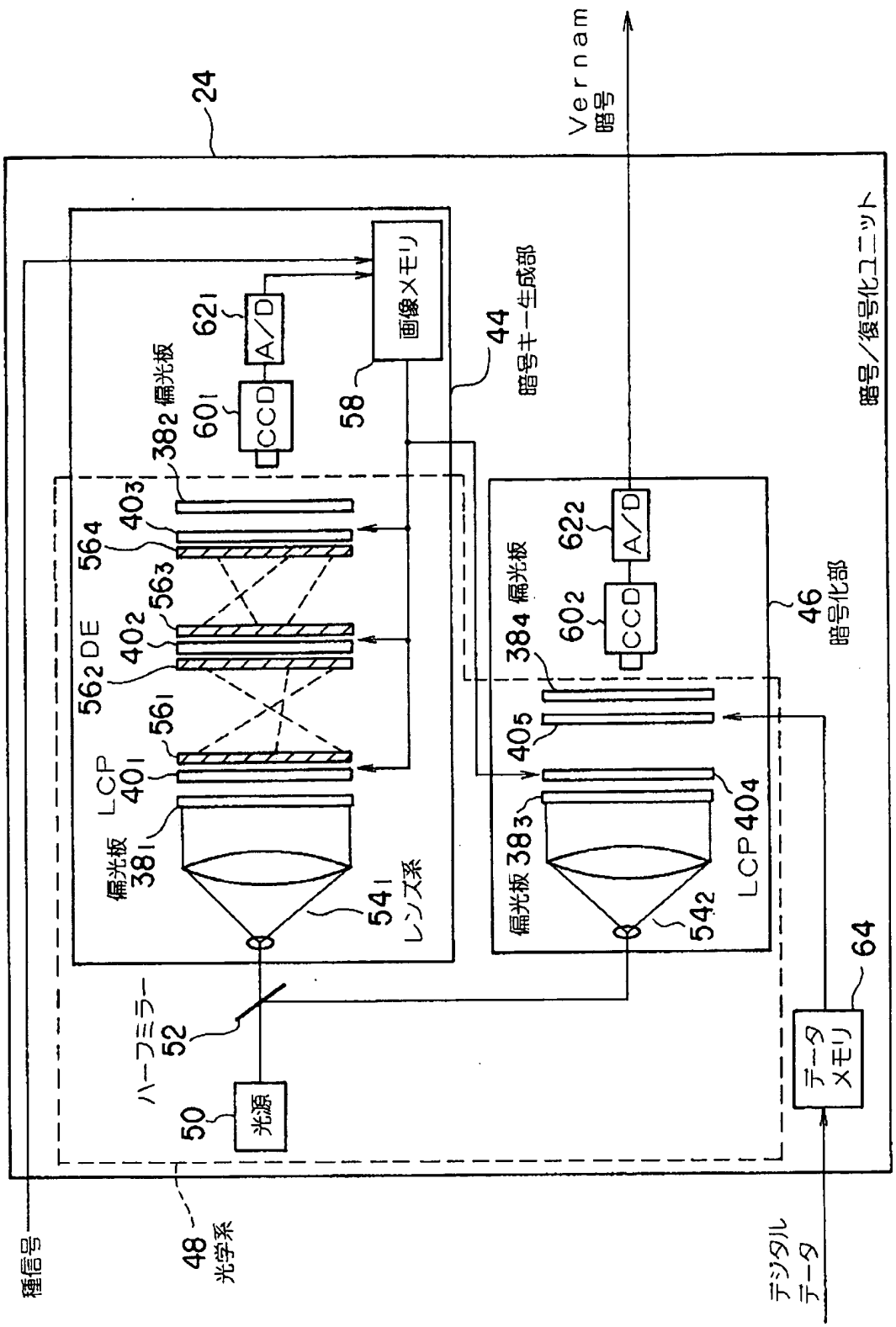
[Translation done.]

Notes:
1. Untranslatable words are replaced with asterisks (****).
2. Texts in the figures are not translated and shown as it is.

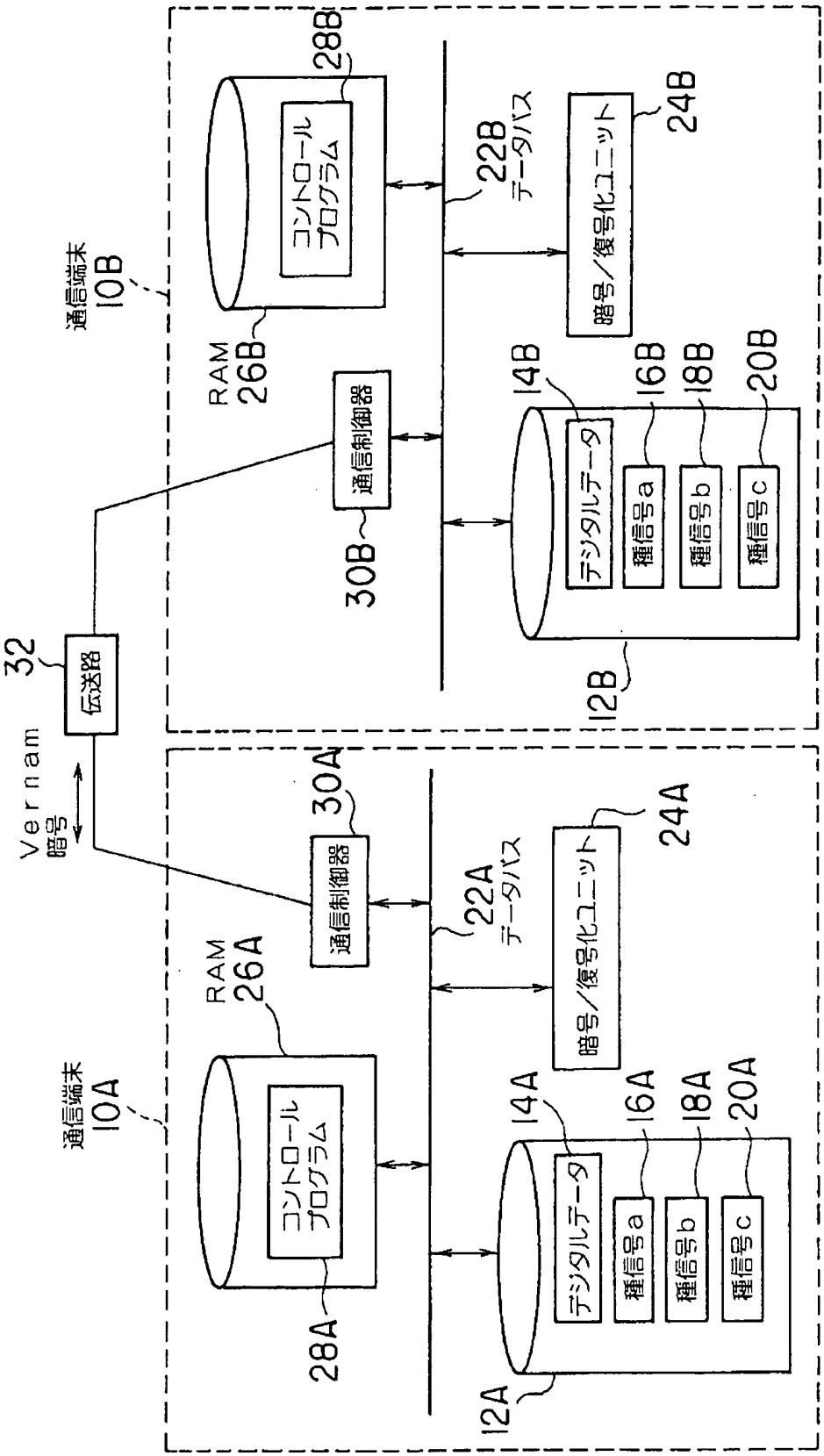
Translated: 00:21:59 JST 02/13/2008
Dictionary: Last updated 01/18/2008 / Priority: 1. Electronic engineering / 2. Mechanical engineering / 3. Mathematics/Physics

[Document Name] Drawings

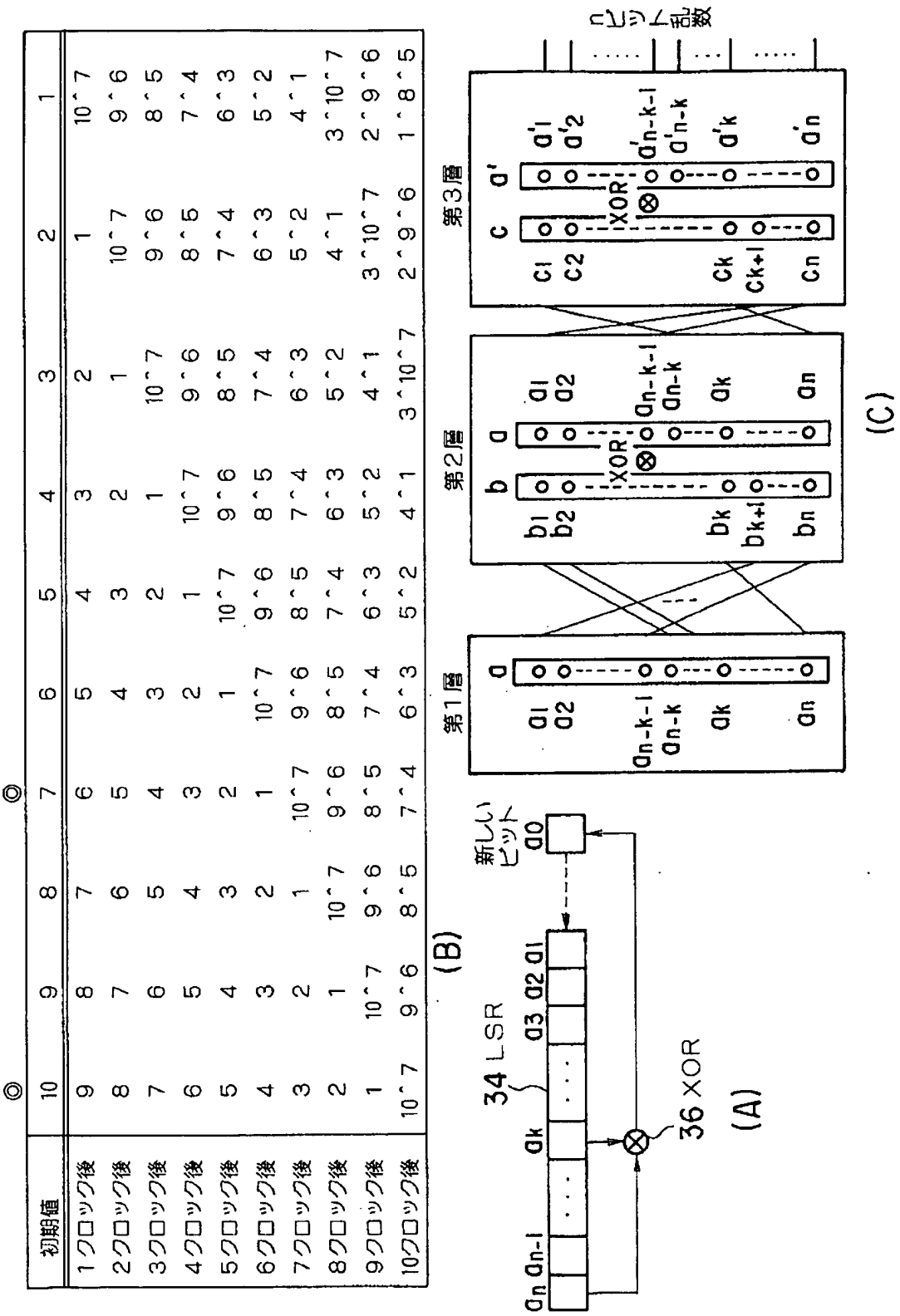
[Drawing 1]


24
Vernam
暗号
暗号/復号化ユニット
画像メモリ
44
暗号キー生成部
A/D
CCD
偏光板
LCP
DE
レンズ系
ハーフミラー
光源
46
暗号化部
データメモリ
64
種信号
48
光学系
デジタルデータ

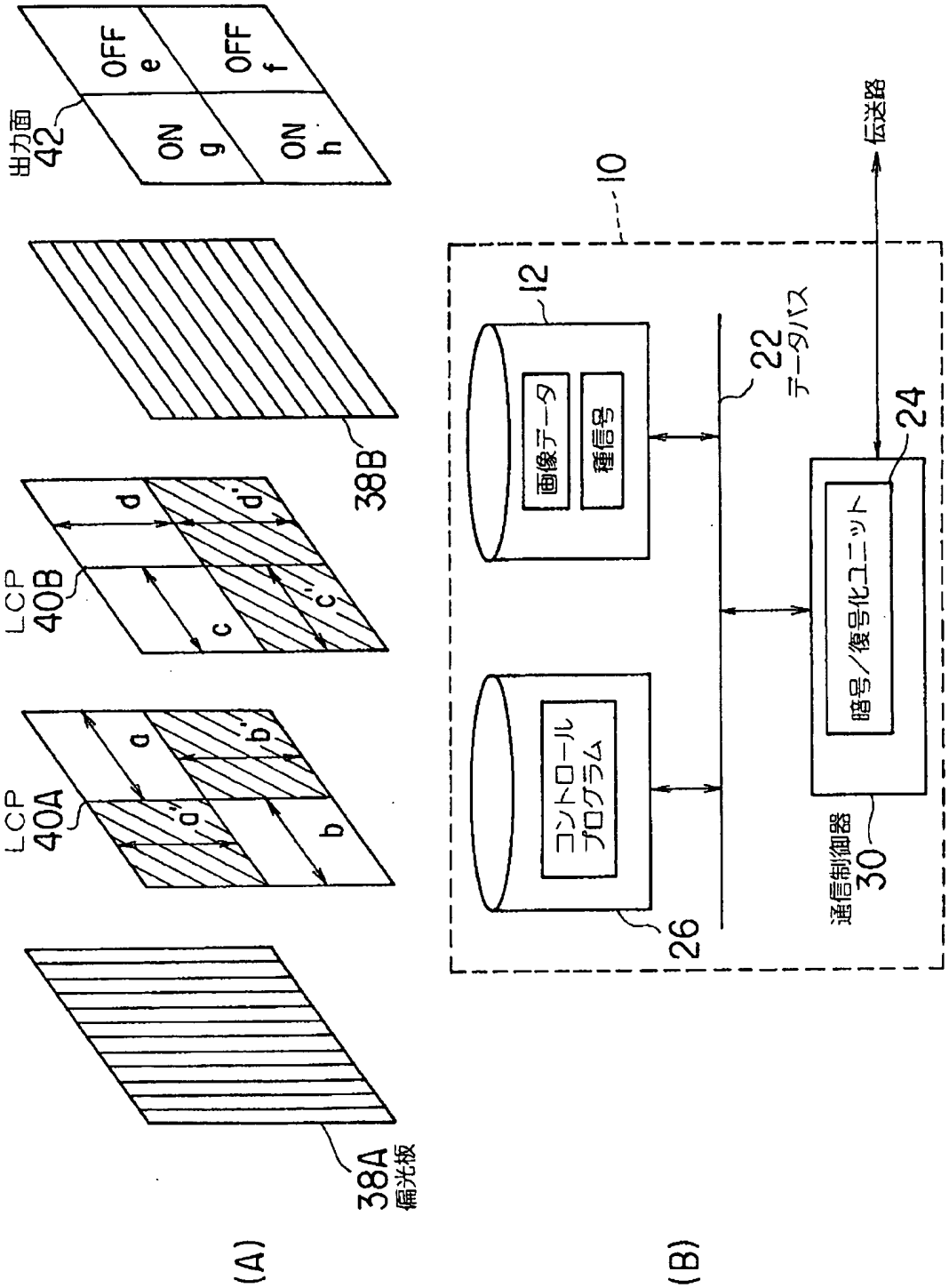
[Drawing 2]


通信端末
10B
28B
コントロール
プログラム
RAM
26B
22B
データバス
暗号／復号化ユニット
24B
通信制御器
30B
14B
16B
18B
20B
デジタルデータ
種信号a
種信号b
種信号c
12B
32
伝送路
Vernam
暗号
通信端末
10A
30A
通信制御器
22A
データバス
24A
暗号／復号化ユニット
RAM
26A
28A
コントロール
プログラム
14A
16A
18A
20A
デジタルデータ
種信号a
種信号b
種信号c
12A

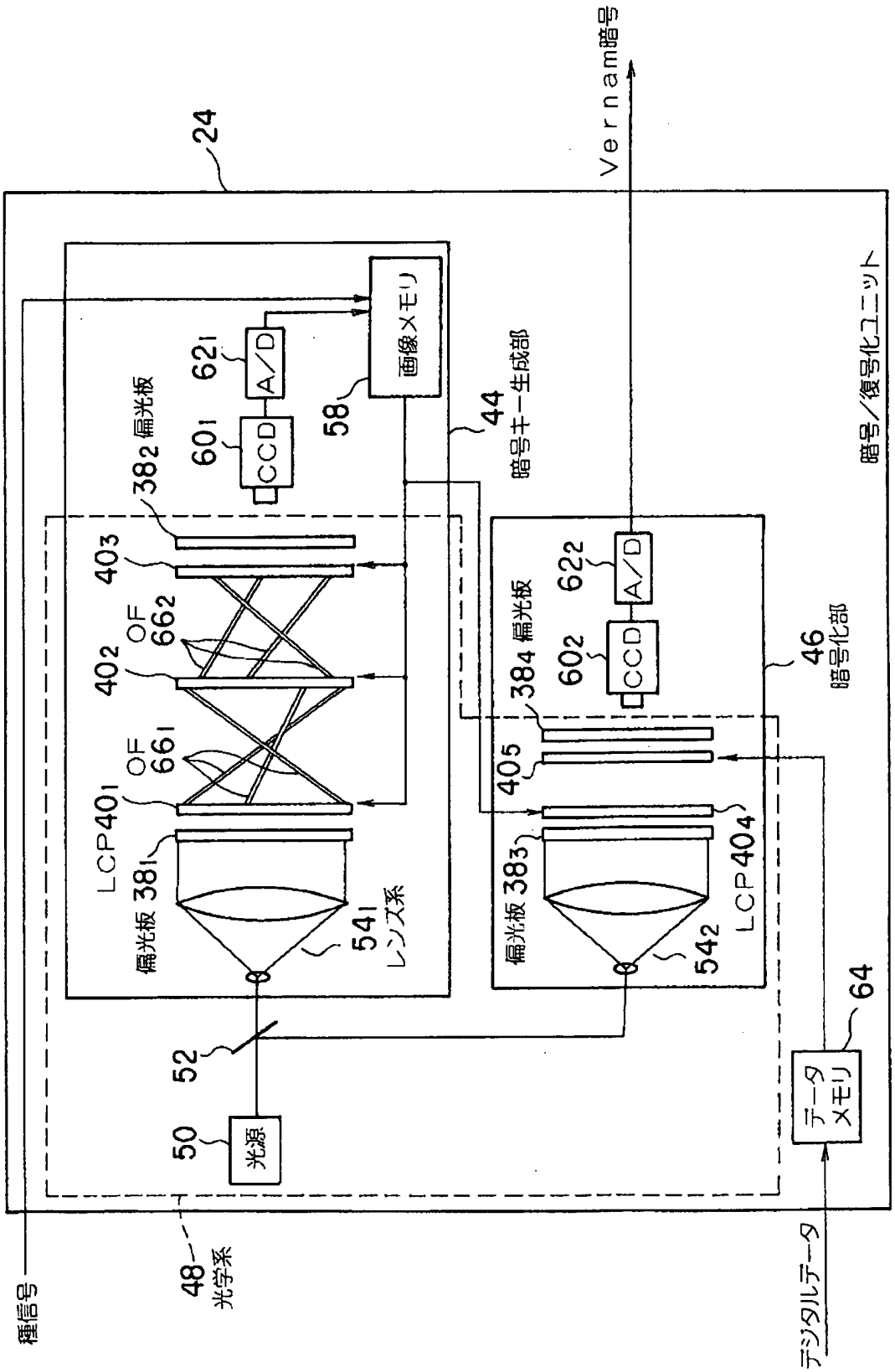
[Drawing 3]


初期値
1クロック後
2クロック後
3クロック後
4クロック後
5クロック後
6クロック後
7クロック後
8クロック後
9クロック後
10クロック後
(B)
34 LSR
36 XOR
(A)
新しいビット
第1層
第2層
第3層
XOR
(C)
クロック数

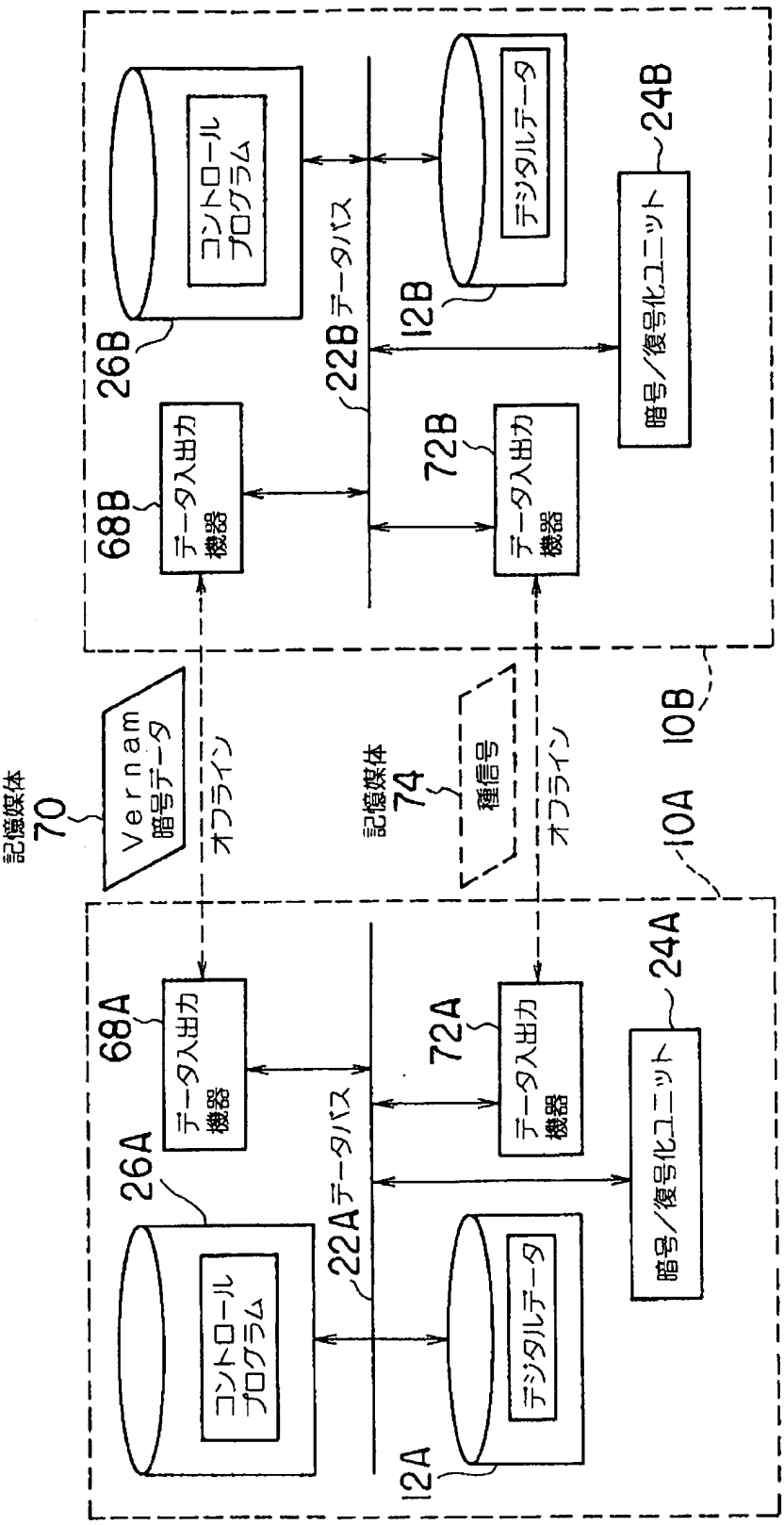
[Drawing 4]


出力面
42
OFF
e
OFF
f
ON
g
ON
h
38B
LCP
40B
d
d'
c
c'
LCP
40A
a
a'
b
b'
38A
偏光板
(A)
10
伝送路
12
画像データ
種信号
22
データバス
24
暗号／復号化ユニット
コントロール
プログラム
26
通信制御器
30
(B)

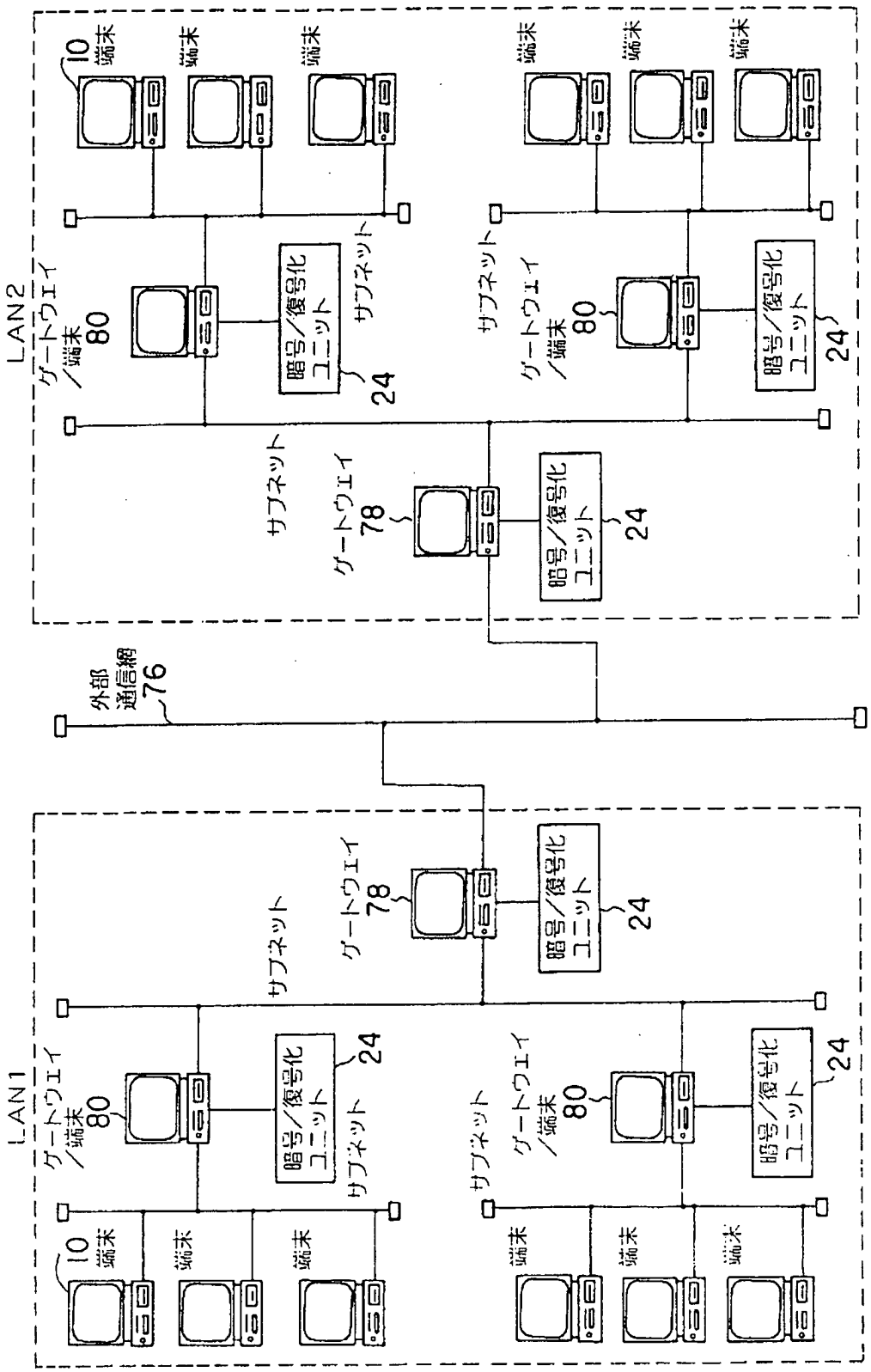
[Drawing 5]


24
Vernam暗号
暗号/復号化ユニット
画像メモリ
A/D
CCD
60_1
62_1
58
44
暗号キー生成部
38_2 偏光板
40_3
OF 66_2
40_2
OF 66_1
40_1
LCP
偏光板 38_1
54_1
レンズ系
38_4 偏光板
60_2
62_2
46
暗号化部
40_5
偏光板 38_3
40_4
LCP
54_2
64
データメモリ
52
50
光源
48
光学系
種信号
デジタルデータ

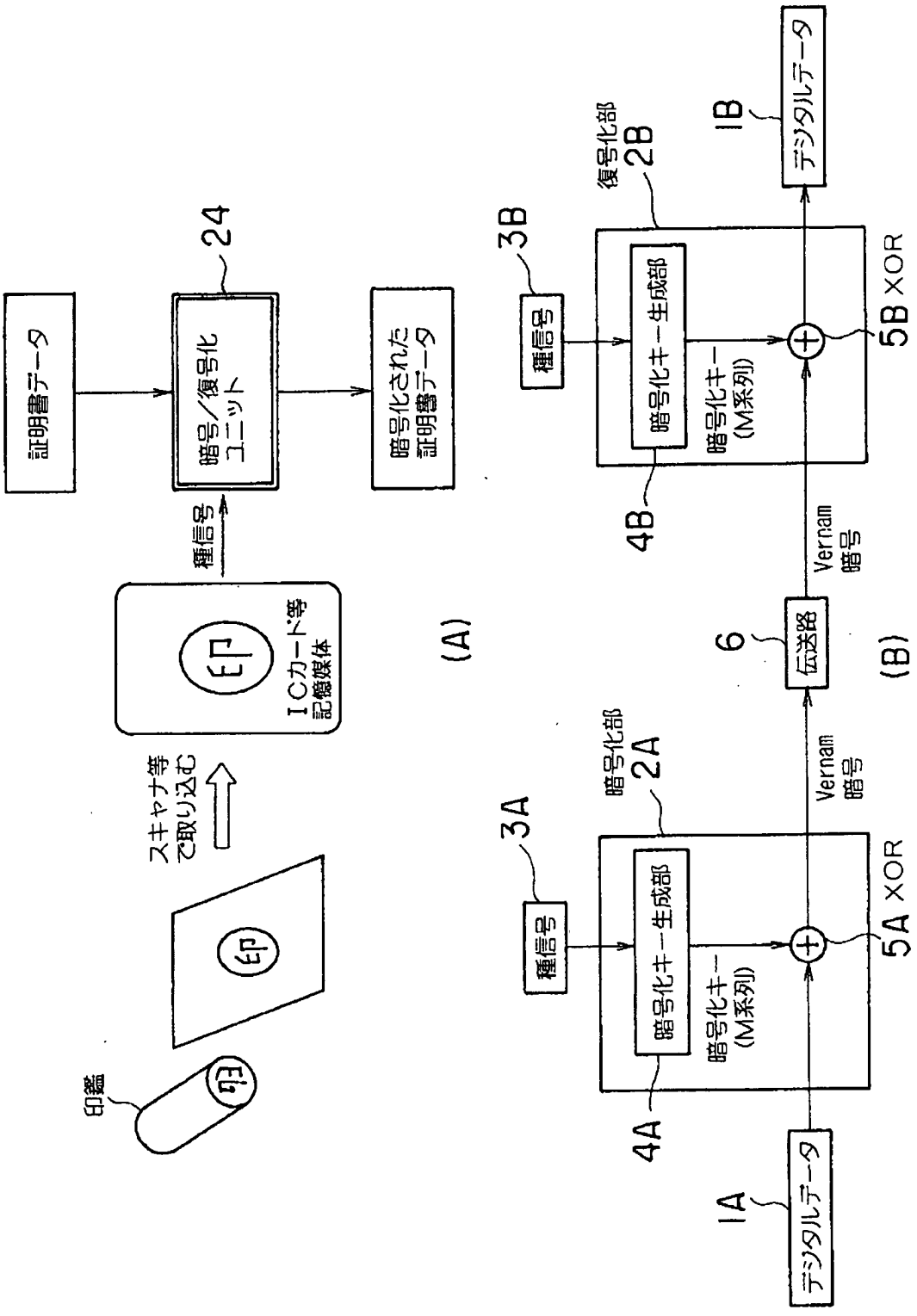
[Drawing 6]


記憶媒体
70
Vernam
暗号データ
オフライン
記憶媒体
74
種信号
オフライン
10B
10A
68B
データ入出力
機器
26B
コントロール
プログラム
22B データバス
72B
データ入出力
機器
12B
デジタルデータ
24B
暗号／復号化ユニット
68A
データ入出力
機器
26A
コントロール
プログラム
22A データバス
72A
データ入出力
機器
12A
デジタルデータ
24A
暗号／復号化ユニット

[Drawing 7]


LAN2
LAN1
外部通信網
76
ゲートウェイ
78
ゲートウェイ／端末
80
サブネット
暗号／復号化ユニット
24
端末
10

[Drawing 8]


証明書データ
24
暗号／復号化
ユニット
暗号化された
証明書データ
種信号
ICカード等
記憶媒体
印
スキャナ等
で取り込む
印鑑
(A)
3B
種信号
暗号化キー生成部
暗号化キー
(M系列)
復号化部
2B
4B
1B
デジタルデータ
5B XOR
Vernam
暗号
6
伝送路
3A
種信号
暗号化キー生成部
暗号化キー
(M系列)
暗号化部
2A
4A
1A
デジタルデータ
5A XOR
Vernam
暗号
(B)

[Translation done.]